CLAIMS

What is claimed is:

1. Apparatus providing one or more computer services for a plurality of customers, the apparatus comprising a real computer on which is set up at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by the respective customer.

2. Apparatus according to claim 1, wherein plural virtual machines are set up within the real computer for at least one of said customers.

3. Apparatus according to claim 1, wherein the or each virtual machine for at least one of said customers is connected to a virtual network set up for said at least one customer within the real computer.

4. Apparatus according to claim 3, comprising a virtual intrusion detection device for detecting an attack on the virtual network.

5. Apparatus according to claim 1, wherein at least one virtual machine is connected to a virtual firewall that is connectable to an external network to which customers and/or other users can connect such that access to said at least one virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

6. Apparatus according to claim 1, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connectable to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

7. Apparatus according to claim 6, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connectable to an external network.

8. Apparatus according to claim 7, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

9. Apparatus according to claim 5, wherein the or at least one of the virtual firewalls is implemented by a virtual machine on the real computer, said virtual firewall virtual machine running firewall software.

10. Apparatus according to claim 1, comprising a plurality of real data storage devices and at least one virtual storage subsystem that is configured to allow said real data storage devices to emulate one or more virtual storage devices.

11. Apparatus according to claim 10, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

12. Apparatus according to claim 10, comprising a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

13. Apparatus according to claim 1, wherein the apparatus is configurable to provide at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple

web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

14. Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

15. Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

16. Apparatus according claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

17. Apparatus according to claim 1, comprising virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

18. Apparatus according claim 1, wherein the real computer comprises plural physical computers.

19. In combination, a first apparatus according to claim 1 and a second apparatus that is substantially identical to said first apparatus, the first and second apparatus being connected by a communications channel so that the second apparatus can provide for redundancy of the first apparatus thereby to provide for disaster recovery if the first apparatus fails.

20. A method of providing one or more computer services for a plurality of customers, the method comprising the steps of:

setting up on a real computer at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification specified by the respective customer.

21. A method according to claim 20, comprising the step of setting up plural virtual machines within the real computer for at least one of said customers.

22. A method according to claim 20, comprising the steps of setting up a virtual network for at least one of said customers within the real computer, and connecting the or each virtual machine for said at least one customer to said virtual network.

23. A method according to claim 22, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

24. A method according to claim 20, comprising the steps of connecting at least one virtual machine to a virtual firewall, and connecting the or each virtual firewall to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

25. A method according to claim 20, comprising the step of connecting the or each virtual machine for a particular customer to a virtual firewall that is dedicated to that customer's virtual machine or machines, and connecting each virtual firewall to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

26. A method according to claim 25, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

27. A method according to claim 26, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

28. A method according to claim 20, comprising the step of configuring at least one virtual storage subsystem to allow multiple real data storage devices to emulate one or more virtual storage devices.

29. A method according to claim 28, comprising the step of configuring the at least one virtual storage subsystem to emulate at least one respective virtual storage device for each customer.

30. A method according to claim 28, comprising the step of using a detection device for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

31. A method according to claim 20, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

32. A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

33. A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

34. A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

35. A method according to claim 20, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

36. A method according to claim 20, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

37. A method of operating a real computer on behalf of plural customers, the method comprising the step of:

operating plural virtual machines on the real computer, each of said plural virtual machines having a specification specified by a respective one of the customers in accordance with a computer service to be provided by the virtual machine on behalf of that customer.

38. A method according to claim 37, comprising the step of operating plural virtual machines within the real computer for at least one of said customers.

39. A method according to claim 37, comprising the step of operating a virtual network for at least one of said customers within the real computer, the or each virtual machine for said at least one customer being connected to said virtual network.

40. A method according to claim 39, comprising the step of using a virtual intrusion detection device for detecting an attack on the virtual network.

41. A method according to claim 37, wherein at least one virtual machine is connected to a virtual firewall, the or each virtual firewall being connected to an external network to which customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall.

42. A method according to claim 37, wherein the or each virtual machine for a particular customer is connected to a virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall being connected to an external network to which each of said customers and/or other users can connect such that access to a virtual machine by a customer or other user via a said external network can only take place through a virtual firewall provided for that virtual machine or machines.

43. A method according to claim 42, wherein each virtual firewall is set up within the real computer, the or each virtual machine for each customer being connected to a first port of the virtual firewall that is dedicated to that customer's virtual machine or machines, each virtual firewall having a second port connected to a virtual network that is set up within the real computer and that is connected to an external network.

44. A method according to claim 43, wherein the second port of each virtual firewall is connected to the same virtual network that is set up within the real computer and that is connectable to an external network.

45. A method according to claim 37, wherein at least one virtual storage subsystem is provided and configured to allow multiple real data storage devices to emulate one or more virtual storage devices.

46. A method according to claim 45, wherein the at least one virtual storage subsystem is configured to emulate at least one respective virtual storage device for each customer.

47. A method according to claim 45, wherein a detection device is used for detecting evidence of malicious software or hostile attack signatures on the at least one virtual storage subsystem.

48. A method according to claim 37, wherein the services provided include at least one of the services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services.

49. A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least some of said virtual machines.

50. A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between at least one virtual machine and an external computer.

51. A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a first virtual network and a second virtual network.

52. A method according to claim 37, comprising the step of using virtual private network software to provide an encrypted communication channel for communication between a virtual network and an external computer.

53. A method according to claim 53, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.

54. A method of providing for a plurality of customers one or more computer services selected from: file, data and archiving services; applications hosting services; database hosting services; data warehouse services; knowledge management hosting services; digital media production services; "intellectual property" and streaming media services; simple web hosting services; complex e-Commerce web hosting services; high performance computation services; electronic messaging and conferencing services; and, learning neuro-computer services; the method comprising the steps of:

setting up on a real computer at the request of each of said customers at least one virtual machine for each of said customers, said at least one virtual machine for each of said customers having a specification determined in accordance with the computer service or services requested by said customer.

55. A method according to claim 54, comprising the step of moving said at least one virtual machine from a first real computer to a second real computer.